Computer Security Incident Response Team Slovakia

CSIRT.SK
www.csirt.gov.sk

November 2010

Agenda

- CSIRT.SK establishing
- Mission statement and goals
- Organization and infrastructure
- Development phases
- Cooperation
- Current activities
- Near future
- Computer incidents
- How to build CSIRT

Information Security in the SR

- **The Ministry of Finance of the Slovak Republic**

(Act No. 275/2006 – Public Administration Information Systems, Non-classified information)

- **National Security Authority**

(Act No. 215/2002 – Electronic signature and Act No. 215/2004 – Classified information)

- **The Ministry of Transport, Posts and Telecommunications of the Slovak Republic**

(Act No. 610/2003 - Electronic communication)

- **The Office for Personal Data Protection**

(Act No. 428/2002 – Personal data protection)

- **The Ministry of the Interior of the Slovak Republic**

(Act No. 300/2005, § 247 – Cybercrime)

- **The Ministry of Economy of the Slovak Republic**

(Act No. 22/2004 – e-Commerce)

- **Telecommunications Office of the Slovak Republic**

(Act No. 610/2003 - Electronic communication)

- **The Ministry of Culture**

(Act. No 618/2003 - Copyright)

- **Ministry of Defense**

And the others …

Establishing a national CSIRT

- The National Strategy for Information Security
  - adopted by Slovak Government under 570/2008

- Ministry of Finance
  - administrative, personnel, technical and financial support

- **CSIRT.SK** has been established
  - as an independent department of DataCentrum
  - on July, 1st. 2009
  - as the first CSIRT/CERT in Slovakia
  - as a **national** / **governmental** CSIRT

Mission Statement

- Response to the IS incidents
  - cooperation with
    - the owners and providers of impacted parts of the national critical infrastructure
    - telecommunication operators
    - ISPs and other public bodies (police, investigators, courts)
- Raising awareness in the field of IS
  - seminars, trainings, best-practices …
- Cooperation and representation
  - international counterparts, peers and organizations

Further Goals

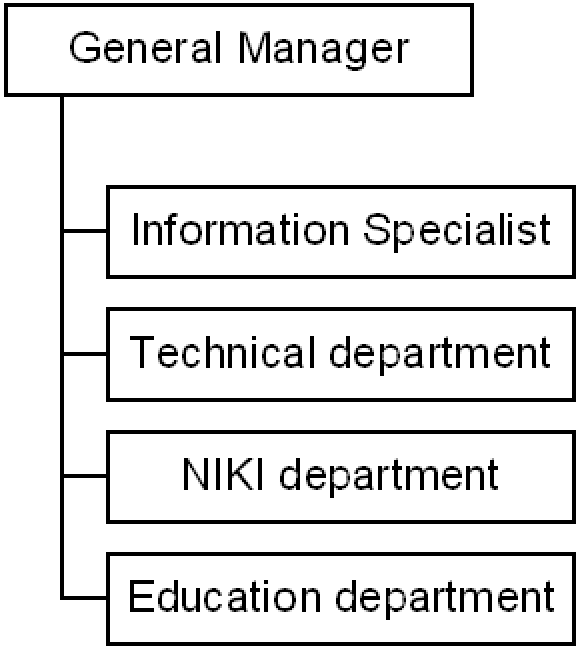
- Contact point
  - National and international warnings
- Monitoring and Information Gathering
  - Level of IS in Slovakia
  - Current threats, vulnerabilities and risks
- Provide services related to IS
  - Reactive / Proactive
- Education and awareness raising
  - IS specialists
  - Users

Further Goals II

- Cooperation with other CSIRT/CERT teams

- At the beginning
  - Only selected services to state administration and later on to the whole public administration

Organization



General Manager

Information Specialist

Technical department

NIKI department

Education department

International cooperation

- ENISA, TERENA
  - Source of information, guide-lines
  - TRANSITS training
- TF-CSIRT
  - Status: “Listed”
- APWG
  - Access to the resources
- CSIRTs/CERTs
  - Czech Republic, Hungary, Poland, Austria, ...
- Cyber Europe 2010

Current Status

- Vulnerability and incident handling
  - via the website from the public
  - web vulnerabilities and phishing
- IS awareness raising and education
  - courses preparation
  - IS terminology
- Incident handling and forensics laboratory
  - HW and SW infrastructure
  - policies, processes
- Information sharing and warning system
  - Central contact and sharing point

Laboratory / Incident handling workspace

- Separated workspaces for improved security and operability
- Structure designed for easy and secure work.
- Tasks:
  - Coordination – operating centre
  - Forensics
  - Incident handling
  - And so on ☺

The future

- Start of providing selected services to selected state and public organizations
- TF-CSIRT – accredited
- FIRST
- Preparing of national exercises
- Cooperation with other CSIRTs in projects
- Full featured forensics laboratory
- …

Computer incidents

Any real or suspected adverse event in relation to the security of computer systems or computer networks

-or-

The act of violating an explicit or implied security policy

Computer incidents

- Classification:
  - Phishing
  - Copyright abuse
  - Intrusion
  - Harassment
  - Web Defacement
  - Spam
  - Malware
  - ....
- Severity
  - Low
  - Medium
  - High

Computer incidents

- Solution ?
  - Proactive
  - Reactive

Reactive solution of computer incidents

- Incident handling
- Manage responsibilities
- Forensics
- Cooperation with law enforcement

Core principles of Incident handling

- Gathering Intelligence
- Understanding the other side
- Monitoring
- Reverse Engineering

- Communication with other relevant subjects (police, courts, commercial companies)
- Communication with IT staff

- **To think.**

Proactive solution of computer incidents

- Announcements and warnings
- IDS / IPS
- Organizational policies
- Rising security awareness / Education of users
- ....

How to build CSIRT/CERT

- Financial issues
- Mission (almost impossible)
- Organizational issues
- Operational issues
- Technical issues
- Legal issues

Organisational issues

- What is competencies of the team ?
  - Can they order to restart server ?
- What is the mission of the team?
  - Proactive
  - Reactive
  - Coordiantional only
- Who is the consituency of the team ?
  - Customers ?
  - Internal employees ?
  - Both ?

Discussion